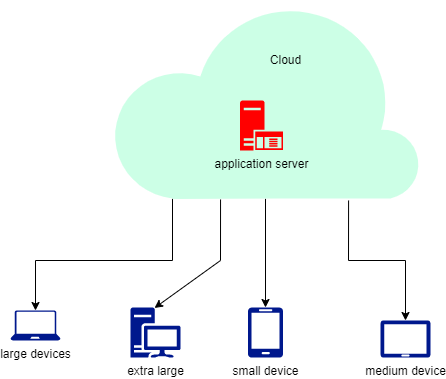
**Network design diagram**

A network design diagram is a diagram that shows how the cloud infrastructure and the web systems have been laid out. The structure is as shown in the following diagram.



**Application/server resource profiles**

The cloud infrastructure for the website will have the following server /application resource files

1. Resource files for small devices that requires an average memory of 32 megabytes and a total of 200 CPU units.
2. Resource files for large devices that requires an average memory of 128 megabytes and a total of 400 CPU units.
3. Resource files for extra large devices that requires an average memory of 320 megabytes and a total of 600 CPU units.
4. Resource files for medium sized devices that requires an average memory of 64 megabytes and a total of 300 CPU units.

**Requirements for cloud deployment**

To ensure that we have a robust infrastructure, the following requirements must be met in the deployment of the cloud strategy

1. Heterogenous system support in that it should have the capacity to support data center existing infrastructure.
2. Service management through resource management and billing cycles.
3. Having real time visibility and reporting capabilities to ensure compliance and security.
4. It should provide interface for end consumers of the service in order to manage their virtual data center and storage.
5. The cloud should have an awareness of workload and resources available.

**Risks and Issues**

1. Unauthorized access to company 0r customer data through the breaches that occur in the cloud platforms.
2. Availability risk – cloud deployment increases the chances that a website may be down since the viability of the enterprise is in the hands of both the cloud vendor and the internet service provider. Bad weather and DDoS attacks can easily affect these two entities hence the website becomes unreliable.
3. There might be compatibility problems between the cloud and the existing IT infrastructure as well as the the policies that are enforced by those seeking the cloud service.

**Firewall Rules**

Application level firewall rule enforces protection of the system against attacks by malicious wares such as viruses. Traffic is filtered based on the content that is being transmitted.

Network level firewall rules inspect packet headers and filters out network traffic based on the IP address of the source and that of the destination and ports that are used.

Stateful multilayer firewall rules filter traffic at the network layer by evaluating packets legitimacy and providing a direct connection between the client and the host.